

Jodi Golinsky  
Vice President &  
Senior Regulatory Counsel

**MasterCard International**

Law Department  
2000 Purchase Street  
Purchase, NY 10577-2509  
914 249-5978  
Fax 914 249-3648  
E-mail [jodi\\_golinsky@mastercard.com](mailto:jodi_golinsky@mastercard.com)  
[www.mastercard.com](http://www.mastercard.com)

*MasterCard  
International*



January 19, 2007

*By Electronic Mail*

Federal Trade Commission  
Office of the Secretary  
Room H-135, Annex N  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

**Re: Identity Theft Task Force, P065410**

To Whom It May Concern:

MasterCard Worldwide ("MasterCard")<sup>1</sup> submits this letter in response to the request for comment issued by the Federal Identity Theft Task Force ("Task Force") and posted on the Federal Trade Commission's ("FTC") Web site on December 26, 2006. The request solicited comments from interested parties regarding a variety of topics in connection with the Task Force's efforts. MasterCard appreciates the opportunity to submit comments for consideration by the Task Force.

MasterCard commends the Task Force for its efforts. Identity theft is a complex issue requiring a multifaceted approach. We are pleased that the Task Force is approaching identity theft from a variety of angles and involving several relevant federal agencies. We applaud such a coordinated approach to this critical issue, and we hope to contribute to the Task Force's ultimate success in proposing a realistic and practical strategy to combat identity theft.

---

<sup>1</sup> MasterCard Worldwide (NYSE:MA) advances global commerce by providing a critical link among financial institutions and millions of businesses, cardholders and merchants worldwide. Through the company's roles as a franchisor, processor and advisor, MasterCard develops and markets secure, convenient and rewarding payment solutions, seamlessly processes more than 16 billion payments each year, and provides industry-leading analysis and consulting services that drive business growth for its banking customers and merchants. With more than one billion cards issued through its family of brands, including MasterCard®, Maestro® and Cirrus®, MasterCard serves consumers and businesses in more than 210 countries and territories, and is a partner to 25,000 of the world's leading financial institutions. With more than 24 million acceptance locations worldwide, no payment card is more widely accepted than MasterCard. For more information go to [www.mastercard.com](http://www.mastercard.com).

We believe the Task Force has an excellent opportunity to review existing efforts by the private and public sector to combat identity theft. Many of these efforts are voluntary, while many are required under existing laws and regulations. The Task Force has the daunting obligation to assemble this information in an effort to propose additional solutions to the problem of identity theft. Given the complexity of the issue and the serious potential for harmful unintended consequences, we applaud the Task Force for requesting public comment on the issue. We urge the Task Force to focus on conceptual approaches and reforms which, once made public, can be more thoroughly debated and considered by additional interested and knowledgeable parties. Our specific comments follow.

### **Use of Social Security Numbers**

We agree with the Task Force's general assessment that the Social Security Number ("SSN") plays an important role in enabling government and private sector entities to have a higher degree of confidence with respect to an individual's identity in an efficient and cost effective way. Without such a unique identifier, it would be difficult to match records across different contexts simply by using a person's name and birth date, or some other type of analogous combination. Simply put, the SSN is an additional verification tool used by the public and private sectors to assist the correct matching of a consumer to his or her records. Moreover, a SSN can be committed to memory easily, much like a home phone number or license plate number, minimizing the need for individuals to carry the number with them and reducing the risk that it will be stolen or misappropriated.

MasterCard recognizes that the SSN can be used by a criminal in an attempt to commit identity theft. The same can be said for names, addresses, and other information used to identify individuals. The solution is not to limit the information available to the public and private sectors for legitimate uses, but to protect such information from misuse. For example, if legitimate and reasonable reliance on SSNs were curtailed, government agencies and companies would have *less* information available to them to verify an individual's identity. If this were the case, it would seem that all an identity thief would need is a phone book (and perhaps knowledge of an individual's birthday) to engage in fraud. Although reliance on SSNs is obviously not foolproof, it does present a meaningful obstacle to identity thieves.

If we are to protect SSNs from misuse it is reasonable to explore ways to reduce unnecessary reliance on the SSN as a unique identifier by all entities, including federal, state, and local governments. This will create fewer opportunities for wrongdoers to access SSNs and reduce their overall circulation. We strongly caution the Task Force, however, that it will be difficult to differentiate between "necessary" and "unnecessary" reliance on, or use of, SSNs. Some reforms may appear obvious, such as not printing SSNs on identification badges. But it is difficult to draw bright lines between legitimate needs for SSNs and frivolous ones.

The Task Force asks for suggestions as to what information could be used as a substitute for SSNs. We are unaware of any other unique, universally recognized identifier

assigned to individuals. Other available unique identifiers include fingerprints and other biometrics, but such information is not widely relied upon in the public or private sector. We believe that if SSNs did not exist, the public and private sector would have simply created a similar unique identification tool, the use of which would pose the same issues posed by reliance on SSNs.

### **Establishing Federal Data Security Standards**

In general, we agree with the Task Force's observation that there is a need to strengthen data security standards for sensitive consumer information, and that a national standard would be the most helpful in addressing any deficiencies in data security practices. At MasterCard, we have already made significant strides in establishing criteria for protecting consumer data with the adoption of the Payment Card Industry Data Security Standard ("PCI Standard"), which applies to all parts of the payment card industry, including merchants and service providers that store, process, or transmit cardholder data. For example, key principles of the PCI Standard include the installation and maintenance of a network firewall and the use of encryption for transmission of cardholder data and sensitive information across public networks. The PCI Standard also requires use of regularly updated anti-virus software, the monitoring of all access to network resources and cardholder data, and the assignment of a unique identification number to persons with computer access to sensitive data.

We believe that the Task Force should recommend flexible standards applicable to all entities that possess sensitive consumer information. The FTC and the federal banking agencies (collectively, "Agencies") were successful in implementing the data security requirements of the Gramm-Leach-Bliley Act ("GLBA") applicable to a wide range of financial institutions with greatly differing levels of compliance resources and sophistication. We believe the Task Force is capable of recommending a similar approach to those entities that possess sensitive consumer information but that are not currently subject to the GLBA information safeguarding requirements.

We recognize that the imposition of information safeguarding requirements on certain private sector companies is not a cost-free proposition. However, we do not believe there is a public policy justification for requiring some entities that possess sensitive consumer information to protect it, while not requiring others to do so. Assuming any new requirement is sufficiently broad and flexible, we do not believe that the costs associated with certain companies developing information safeguarding programs would outweigh the benefits of the requirement. To the extent the Task Force is interested in reviewing the impact such a proposal may have on smaller, less sophisticated entities, we believe the FTC should have such information as a result of its imposition of the GLBA requirements on a variety of smaller financial institutions.

### **Establishing Federal Breach Notice Requirements**

MasterCard supports efforts to establish an appropriate national data breach notice standard. We strongly believe that any national standard should: (i) have an appropriate "trigger" before notices are sent; (ii) establish a uniform national standard; (iii) be enforced

solely by the functional regulators; and (iv) recognize the sufficiency of existing data breach guidance issued by the federal banking agencies under the GLBA. We believe that it is critical that any data breach notification requirement be predicated on the determination that affected consumers face substantial risk of harm as a result of the data breach. Sending consumers notices when they are not at risk only increases the likelihood that breach notices lose their significance to consumers, becoming the equivalent of “crying wolf” too many times. We also believe that there should be a national uniform standard with respect to data breach notices, ensuring that this inherently interstate issue receives uniform and meaningful treatment. The determination of whether to send a notice should not be subject to second guessing by the trial bar. Rather, the requirements should be enforced in a uniform manner by the federal functional regulators. Finally, we believe that the GLBA data breach notice requirements generally provide a reasonable framework of consumer protections, and that financial institutions should not be required to develop another compliance program. Rather, financial institutions who comply with the GLBA data breach notice guidance should be deemed to be in compliance with any new federal notification requirement.

### **Preventing the Misuse of Consumer Data**

MasterCard strongly supports efforts to prevent the misuse of consumer data and applauds the Task Force on its efforts to consider measures that would make it more difficult for identity thieves to use misappropriated information to steal identities. We believe that the Task Force’s intention to hold a series of workshops would be useful in exploring tactics and strategies that public and private sector entities have used successfully. This will also give the Task Force the opportunity to take a partial inventory with respect to existing legal and regulatory requirements, complete with feedback on their utility. Understanding and evaluating existing and forthcoming efforts and requirements is an important component of the Task Force’s work. It is not as though the private sector does not take serious precautions against identity theft, either voluntarily or pursuant to law. The Task Force should take the opportunity to learn about what is happening in the marketplace and proceed with the benefit of that knowledge. For example, many financial institutions are subject to regulations issued under Section 326 of the USA PATRIOT Act. Although these regulations were designed to play a role against terrorism, they have an obvious impact on identity theft prevention. We also note that the Agencies recently proposed, but have yet to finalize, a “red flags” rule that would require each financial institution and creditor to develop and implement an identity theft prevention program (“Red Flag Proposal”). *See* 71 Fed. Reg. 40786 (July 18, 2006). We believe it would be important for the Task Force and others to learn about experiences with these types of requirements and how to build from them.

### **Financial Institutions Assisting Victims and Law Enforcement**

We agree with the Task Force’s intentions to improve identity theft mitigation measures for victims. To that end, we generally agree that financial institutions can be an important source of information for law enforcement seeking to prosecute identity theft, as well as for individuals seeking to remedy the effects of an identity theft. In addition, it is important to recognize that financial institutions are also the victims of identity theft, as

they bear the monetary losses associated with many types of identity theft. It is in everyone's interest to prevent, investigate, and mitigate identity theft.

We note that the Task Force has inquired whether the Justice Department should initiate discussions with the private sector to encourage increased public awareness of Section 609(e) of the Fair Credit Reporting Act ("FCRA"). As a primary matter, it is not clear to us whether the Justice Department should be involved in consumer education pertaining to the rights of identity theft victims, or whether this should be the function of the FTC. Furthermore, victims of identity theft are *already* informed of their rights under Section 609(e) pursuant to existing disclosure requirements imposed on consumer reporting agencies. To the extent that consumer education with respect to Section 609(e) should be improved, we ask the Task Force to consider the issue in the broader context of educating victims with respect to all of their rights. For example, we do not believe that the rights granted under Section 609(e) of the FCRA are necessarily more (or less) important than other rights. We also believe that victims should be aware of the limitations inherent in Section 609(e), and that victims do not have an absolute right to information. These limitations are important to guard against criminals posing as victims and obtaining information about innocent consumers.

### **Prosecuting Identity Theft and Other Law Enforcement Issues**

MasterCard strongly supports the efforts of law enforcement to combat identity theft. We have a strong record of working with law enforcement in connection with financial crimes, and we believe that law enforcement needs additional monetary resources to fight identity theft. To the extent criminal laws need revision to assist law enforcement in apprehending and prosecuting identity thieves, we support the Task Force's consideration of these matters.

The Task Force also solicits comment on whether the Justice Department should initiate discussions with consumer reporting agencies "on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report." To the extent discussions with the private sector are necessary on this topic, they should be with the credit grantors. Consumer reporting agencies are simply information repositories—consumer reporting agencies do not have a role in deciding who receives credit. Furthermore, we believe that this issue has been handled in the past by the federal banking agencies through formal and informal means, including regulations. This is an example of where it may be useful for the Task Force's proposed symposia to provide further understanding of how PATRIOT Act, FACT Act, and other regulations come together and whether any weaknesses could be addressed.

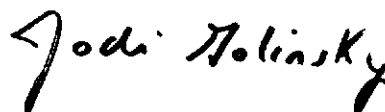
The Task Force also proposed to offer legislation that would make it a felony for "data brokers and telephone company employees to knowingly and intentionally sell or transfer customer information without prior written authorization from the customer, with appropriate exceptions for law enforcement purposes." MasterCard strongly cautions the Task Force to consider the ramifications of this proposal. The plain language of the concept could eliminate a variety of activities, including the consumer reporting industry, the ability to sell financial accounts, and the ability to engage in fraud prevention. We also

urge the Task Force to consider whether sources of information used by law enforcement would disappear as a result of the elimination of any viable business purpose for them.

\* \* \* \* \*

Once again, we appreciate the opportunity to comment on the Task Force's recommendations. If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me, at the number indicated above, or Michael F. McEneney at Sidley Austin LLP, at (202) 736-8368, our counsel in connection with this matter.

Sincerely,

A handwritten signature in black ink that reads "Jodi Golinsky". The signature is written in a cursive, slightly stylized font.

Jodi Golinsky  
Vice President &  
Regulatory and Public Policy Counsel

cc: Michael F. McEneney, Esq.